Exhibit A

University at Buffalo
Clinical Legal Education
School of Law

September 10, 2018

Federal Bureau of Investigation
Attn: FOI/PA Request
Record/Information Dissemination Section
170 Marcel Drive
Winchester, VA 22602-4843
Fax: (540) 868-4391/4997

Drug Enforcement Administration
Attn: FOI/PA Unit (SARF)
8701 Morrissette Drive
Springfield, Virginia 22152
Email: DEA.FOIA@usdoj.gov

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street, S.W., Stop 5009
Washington, D.C. 20536-5009
Fax: (202) 732-4265

U.S. Customs and Border Protection
FOIA Officer
90 K Street, NW
9th Floor, Mail Stop 1181
Washington, D.C. 20229

U.S. Secret Service
Communications Center (FOIA/PA)
245 Murray Lane
Building T-5
Washington, D.C. 20223
Email: FOIA@usss.dhs.gov

Amanda Marchand Jones, Chief
FOIA/PA Unit
Criminal Division
Department of Justice
Suite 1127, Keeney Building
Washington, DC 20530-0001
Email: crm.foia@usdoj.gov

Internal Revenue Service
Central Processing Unit
Stop 211
PO Box 621506
Atlanta, GA 30362-3006
Fax: (877) 807-9215

RE: Expedited FOIA Request
Law Enforcement Hacking

Dear FOIA Officer:

We write on behalf of Privacy International ("PI"), the American Civil Liberties Union and American Civil Liberties Union Foundation (together, the "ACLU"), and the University at Buffalo School of Law Civil Liberties and Transparency Clinic ("CLTC") to

507 O'Brian Hall, Buffalo, NY 14260-1100
716.645.6222 (F) 716.645-2167
jmmanes@buffalo.edu

www.law.buffalo.edu/clinics

request the disclosure of records pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, regarding the government's use of hacking for investigative purposes.[1]

I. Background

Law enforcement officials in the federal government have used hacking techniques to interfere with computer systems so as to access and gather sensitive information, including individuals' locations, internet activities, communications, and personal files. The use of these techniques therefore raises significant privacy concerns and may violate U.S. as well as international law. We make this request to seek further information regarding law enforcement use and regulation of hacking, including: (1) how often, and under what circumstances, government actors use these techniques to investigate civilians; (2) what internal rules govern these techniques; and (3) what consideration has been given to the legality of these techniques.

Law Enforcement Hacking

Hacking refers to an act or series of acts, which interfere with a computer system, causing it to act in a manner unintended or unforeseen by the manufacturer, user or owner of that system.[2] Government hacking for surveillance seeks to identify and exploit such vulnerabilities, not to secure systems, but to facilitate a surveillance objective (*i.e.* to gather

---

[1] Privacy International is a United Kingdom-based non-profit organization, which defends the right to privacy around the world. Privacy International undertakes research and investigations into government and corporate surveillance with a focus on the laws, policies and technologies that enable these practices. It litigates cases implicating the right to privacy in the courts of the U.S., the United Kingdom, and Europe. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional, and international laws that protect this fundamental right. As a part of this mission, Privacy International works with various partner organizations around the world to identify and address threats to privacy. Privacy International, *About Privacy International*, https://www.privacyinternational.org/about (last visited Mar. 15, 2018).

The American Civil Liberties Union Foundation is a 26 U.S.C. § 501(c)(3) organization that provides legal representation free of charge to individuals and organizations in civil rights and civil liberties cases, educates the public about civil rights and civil liberties issues across the country, directly lobbies legislators, and mobilizes the American Civil Liberties Union's members to lobby their legislators. The American Civil Liberties Union is a separate non-profit, 26 U.S.C. § 501(c)(4) membership organization that educates the public about the civil liberties implications of pending and proposed state and federal legislation, provides analysis of pending and proposed legislation, directly lobbies legislators, and mobilizes its members to lobby their legislators.

CLTC is a legal clinic that conducts litigation and policy advocacy to pursue government transparency, democratic accountability and the protection of individual rights, especially free speech, privacy, and other basic constitutional protections.

[2] In computing terms, hacking originally described the hobby of computer programming and encompassed the idea of finding creative solutions to technology problems. The term gradually evolved to describe the activity of finding vulnerabilities in computer security, first with the goal of reporting or repairing them, but later also to exploit them for other purposes.

evidence or intelligence or to assist the evidence of intelligence-gathering process). U.S. government actors have referred to hacking using various other terms, such as "computer network exploitation" ("CNE") or "network investigative technique" ("NIT").[3] This request uses the term "hacking" to refer to all techniques designed to interfere with computer systems, regardless of how they are described by the government.

Hacking can permit remote access to computer systems and therefore potentially to all of the data stored on those systems. This activity is very privacy-intrusive because, for an increasing number of people, their laptops and cell phones contain the most private information they store anywhere. Hacking can also permit governments to conduct novel forms of real-time surveillance, by covertly turning on a device's microphone, camera or GPS-based locator technology. The information gathered through hacking can allow a government actor to build a complete profile of a person or reveal a person's most intimate thoughts. Such information can include details about a person's movements, communications, internet searches, personal files, and other private data.

As part of its hacking operations, the government often relies on social engineering, which involves tricking or manipulating an individual into performing a specific action. Because social engineering is often used as a method of interfering with systems, this request defines certain social engineering techniques to constitute a form of hacking. Phishing, for example, is a common social engineering technique involving the impersonation of a reputable person or organization. Phishing attacks typically take the form of an email or text message, which may contain a link or attachment infected with malicious software ("malware"). Because the sender appears to be a trusted third party, the recipient is likely to click on the infected link or attachment, which then installs malware on the recipient's device.

Law enforcement officials have been known to use a wide variety of hacking and related social engineering techniques. These techniques may be designed to "covertly download files, photographs and stored emails, or even gather real-time images by activating cameras connected to computers."[4] Others are designed to monitor and intercept communications, including by logging keystrokes on a target device.[5] One technique,

---

[3] *See* Kim Zetter, *Hacker Lexicon: What Are CNE and CNA?*, Wired, July 6, 2016, https://www.wired.com/2016/07/hacker-lexicon-cne-cna/; Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, Wash. Post, Dec. 6, 2013, https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html?utm_term=.ecbf9739498d.

[4] Timberg & Nakashima, FBI's Search for 'Mo,' *supra* note 3.

[5] *See, e.*g., Kim Zetter, *Everything We Know About How the FBI Hacks People,* Wired, May 15, 2016, https://www.wired.com/2016/05/history-fbis-hacking/; In Re Warrant to Search a Targeted Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).

commonly known as a "watering hole attack," can be used on hundreds or thousands of computers at a time, reporting certain activity and information back to law enforcement. The FBI has commandeered and operated websites, using a "watering hole" attack to covertly deliver malware to thousands of visitors around the world.[6] Law enforcement has also used social engineering techniques like phishing to deliver malware.[7]

Law enforcement officials sometimes also purchase or borrow tools that enable them to deploy hacking techniques. Privacy International has identified over 500 surveillance technology companies that sell products and services exclusively to government clients for law enforcement and intelligence-gathering purposes,[8] including tools to enable hacking. According to one company that sells hacking tools, such techniques can provide "full access to stored information with the ability to take control of [a] target system's functions to the point of capturing encrypted data and communications."[9] Off-the-shelf software packages now make it possible for many different types of law enforcement agencies – ranging in technical sophistication – to deploy hacking techniques.

The extent of law enforcement agencies' use of hacking tools is largely unknown to the public, but reports suggest that their use is expanding.[10] The FBI, for example, spent

---

[6] *See* American Civil Liberties Union et al., *Challenging Government Hacking in Criminal Cases*, 1, https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf; Zetter, *Everything We Know About How the FBI Hacks People*, *supra* note 5.

[7] *See, e.g.*, Raphael Satter, *How a School Bomb-Scare Case Sparked a Media vs. FBI Fight,* Associated Press, Mar. 18, 2017, https://www.ap.org/ap-in-the-news/2017/how-a-school-bomb-scare-case-sparked-a-media-vs.-fbi-fight.

[8] Privacy International, *Privacy International Launches the Surveillance Industry Index & New Accompanying Report*, Oct. 23, 2017, https://www.privacyinternational.org/blog/54/privacy-international-launches-surveillance-industry-index-new-accompanying-report (last visited July 18, 2018).

[9] *FinFisher: Governmental IT Intrusion and Remote Monitoring Solutions*, 12, https://www.documentcloud.org/documents/408444- (last visited July 18, 2018).

[10] There are now numerous examples of commercially-available equipment, software and/or technology for hacking including but not limited to: Remote Control System a.k.a. RCS or Galileo (marketed by Hacking Team); Finfisher, FinFisher Relay, FinSpy, and FinFly (marketed by Lench IT Solutions); Pegasus (marketed by NSO Group), and various tools marketed by VUPEN Security. For more information about various commercial hacking tools, see Wall St. J., *The Surveillance Catalog: How Government Gets Their Tools*, http://graphics.wsj.com/surveillance-catalog/; Surveillance Industry Index, https://sii.transparencytoolkit.org/.

Various government agencies, predominantly the intelligence agencies, have also developed their own "equipment, software and/or technology" in-house. Government-developed tools include but are not limited to the following: OutlawCountry, Quantum Insert, ELSA, Pandemic, VALIDATOR, CAPTIVATEDAUDIENCE, GUMFISH, GROK, FOGGYBOTTOM, SALVAGERABBIT, UNITEDRAKE, Double Pulsar, FEEDTROUGH, and CIPAV (developed by the FBI). *See, e.g.,* Swati Khandelwal, *Shadow Brokers Leaks Another Windows Hacking Tool Stolen from NSA's Arsenal*, The Hacker News, Sep. 07, 2017, https://thehackernews.com/2017/09/shadowbrokers-unitedrake-hacking.html; Swati Khandelwal, *Wikileaks Reveals CIA Malware that Hacks and Spy on Linux Computers*, The Hacker News, June 30, 2017, https://thehackernews.com/2017/06/cia-linux-hacking-tool-malware.html; Kim Zetter, *How to Detect Sneaky*

more than $1 million on software to hack into a locked iPhone in a single case, and has indicated that it will continue to invest in such technology.[11] A recent report from the Office of Inspector General for the Department of Justice discloses that the FBI has used classified hacking tools, typically reserved for matters of national security, in ordinary criminal cases.[12] Immigration and Customs Enforcement has reportedly purchased $2 million of "some of the most powerful phone and laptop hacking technology available" from Israeli company Cellebrite,[13] in addition to "record sums" spent with other surveillance technology companies selling hacking tools.[14] Similarly, the Drug Enforcement Agency ("DEA") has expressed interest in hacking tools produced by NSO Group, according to documents obtained in response to a FOIA request.[15] NSO Group is a "leader in the field of Cyber warfare," whose products have been linked to hacking attempts on journalists and activists in other countries.[16] According to a promotional brochure, NSO Group describes Pegasus – a form of malware produced by the company – as "a powerful and unique monitoring tool . . . [w]hich allows remote and stealth monitoring and full data extraction from remote target

---

NSA 'Quantum Insert' Attacks, Wired, Apr. 22, 2015, https://www.wired.com/2015/04/researchers-uncover-method-detect-nsa-quantum-insert-hacks/; Jacob Appelbaum et al., *NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need*, Spiegel Online, Dec. 30, 2013, http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006-druck.html; Jacob Appelbaum et al., *Catalog Advertises NSA Toolbox,* Spiegel Online, Dec. 29, 2013, http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006-druck.html; Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware,* Electronic Frontier Foundation, Apr. 29, 2011, https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav.

[11] Janus Kopfstein, *FBI Director: We Paid More Than $1.2 Million for San Bernardino iPhone Hack,* Motherboad, Apr. 21, 2016, https://motherboard.vice.com/en_us/article/9a3kn5/fbi-director-we-paid-more-than-1-2-million-for-san-bernardino-iphone-hack; Ellen Nakashima, *Comey Defends FBI's Purchase of iPhone Hacking Tool,* Wash. Post, May 11, 2016, https://www.washingtonpost.com/world/national-security/comey-defends-fbis-purchase-of-iphone-hacking-tool/2016/05/11/ce7eae54-1616-11e6-924d-838753295f9a_story.html?utm_term=.5905627cd806.

[12] Joseph Cox, *The FBI Used Classified Hacking Tools in Ordinary Criminal Investigations*, Motherboard, Mar. 29, 2018, https://motherboard.vice.com/en_us/article/7xdxg9/fbi-hacking-investigations-classified-remote-operations-unit; Office of the Inspector General for the U.S. Department of Justice, *Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation*, Mar. 2018, https://oig.justice.gov/reports/2018/o1803.pdf.

[13] Thomas Fox-Brewster, *US Immigration Splurged $2.2 Million on Phone Hacking Tech Just After Trump's Travel Ban*, Forbes, Apr. 13, 2017, https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/#36a0512aa1fc.

[14] *Id*. Other suppliers include Oxygen Forensics based in Russia and Magnet Forensics based in Canada.

[15] Joseph Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, Motherboard, Aug. 2, 2017, https://motherboard.vice.com/en_us/article/gygxk9/the-dea-met-with-controversial-iphone-hackers-nso-group.

[16] *Id*.

devices via untraceable commands."[17] DEA has also reportedly spent almost $1 million on similar technology sold by the Italian surveillance technology company, Hacking Team.[18] Even local law enforcement agencies across the country have access to relatively cheap hacking tools, in some cases costing only $50 to hack an iPhone.[19]

Concerns Raised by Hacking

Law enforcement use of hacking presents unique and grave threats to our privacy and security. With respect to privacy, as discussed above, hacking is a particularly intrusive technique, permitting both remote access to systems as well as novel forms of real-time surveillance. In addition, hacking raises especially significant concerns about particularity and minimization. In certain circumstances, government actors may use hacking techniques where they lack information regarding the identity of the targeted person and/or the device(s) of that person – for example, where a target person uses technology to protect their anonymity or secure their information.[20] Moreover, modern digital devices can be used by multiple users (or permit multiple user profiles, which can correspond to one or more users), making it difficult for government actors to pinpoint with accuracy the target person. Modern devices also permit users to access or store many different kinds of intimate information and to communicate in many different ways. In this context, it is especially crucial to establish special minimization procedures that limit access to and collection of information; such limits will be essential in order to comply with constitutional, statutory, and even international human rights principles.

Law enforcement use of hacking is equally concerning from a security perspective. Hacking can not only undermine the security of a target device – by exploiting a security vulnerability – but also of other systems in a number of ways. The government's use of malware might proliferate to systems beyond the target device. More broadly speaking, its exploitation of a particular vulnerability is a choice to perpetuate the insecurity of a system, which many individuals may use, and may therefore be susceptible to similar attacks by other actors. Social engineering techniques, when used in conjunction with hacking, can also

---

[17] NSO Group promotional brochure, available at https://www.documentcloud.org/documents/815991-1276-nso-group-brochure-pegasus.html.

[18] Cox, The DEA Met with Controversial iPhone Hackers NSO Group, *supra* note 15.

[19] Joseph Cox, *Cops Around the Country Can Now Unlock iPhones, Records Show*, Motherboard, Apr. 12, 2018, https://motherboard.vice.com/en_us/article/vbxxxd/unloc-iphone-ios11-graykey-grayshift-police.

[20] One example is the FBI's "Freedom Hosting" operation, where the FBI deployed a "watering hole attack" on the servers of the Freedom Hosting service. The FBI turned each server into a watering hole and subsequently infected with malware any device that visited the server whether or not that device was of interest to the FBI. Kevin Poulsen, *FBI Admits it Controlled TOR Servers Behind Mass Malware Attack,* Wired, Sept. 13, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi/.

threaten security by eroding the trust users place in their communications with third parties, which is critical to maintaining the security of systems and the internet as a whole.[21]

Law enforcement use of hacking also creates significant potential for misuse. Like other forms of surveillance, government actors wield these techniques surreptitiously, but they can also wield them remotely and at scale. A single hacking operation can sweep up individuals incidental or unrelated to a government investigation. Hacking also permits the manipulation of data in a world that is increasingly data-driven. Through hacking, governments may, for instance, intentionally or unintentionally delete, corrupt or plant data, which raises concerns about the integrity of any evidence gathered using these techniques. Moreover, because hacking involves highly technical methods that can require significant subject-matter expertise to understand, judicial oversight of such techniques is especially difficult.

In light of the privacy and security implications of hacking tools, as well as their potential for misuse, these techniques should be subject to clear, public rules. At present, however, it is unclear what rules govern the use of hacking and related social engineering techniques by law enforcement. Under U.S. law, where the government seeks access to stored content a warrant is ordinarily required and must be founded upon probable cause that the stored information will contain evidence of a crime.[22] Where the government seeks to intercept the content of communications in real time, the law generally requires a warrant founded upon probable cause not just that a person has committed or will commit a crime, but also that the targeted communication channels will be used in connection with the crime or are owned by the target.[23] More broadly, "searches and seizures" must comply with the Fourth Amendment's "reasonableness" requirement, which generally requires a warrant. Warrants, in turn, can be issued only upon a finding of probable cause and only when they describe with particularity the places or things to be searched or seized.[24]

---

[21] *See generally How Malicious Software Updates Endanger Everyone*, ACLU, https://www.aclu.org/issues/privacy-technology/consumer-privacy/how-malicious-software-updates-endanger-everyone (last visited Aug. 6, 2018). For example, in the "Timberline" case, the FBI impersonated a journalist from the Associated Press ("AP") who sent malware-embedded links to a fake AP article online to a teenager suspected of calling fake bomb threats to his school. When the operation came to light, the AP strongly denounced the FBI's appropriation of its identity for investigative purposes. Records disclosed in a subsequent FOIA lawsuit brought by the AP reveal that the FBI may have violated its own guidelines in using the social engineering technique in this case. Satter, *How a School Bomb-Scare Case Sparked a Media vs. FBI Fight*, *supra* note 7.

[22] 18 U.S.C. § 2703 (2017) (stating that stored content can be accessed via subpoena or court order in addition to a warrant, but under different requirements, including prior notice).

[23] 18 U.S.C. § 2518 (2017).

[24] U.S. Const., amend. IV.

Yet, it is unclear whether and when law enforcement agencies regard hacking and related social engineering techniques as subject to these warrant requirements. It is also unclear whether and when law enforcement believes such techniques can be used with judicial authorization short of a warrant,[25] or with no prior authorization at all.[26] In addition, little is known about the internal rules that law enforcement agencies have adopted to regulate the deployment of hacking and related social engineering techniques by agency officials.

Without more information, the public is not able to understand and effectively regulate the government's use of hacking and related social engineering techniques. The public should be able to know what hacking techniques are being deployed by their law enforcement agencies and what information can be acquired using such techniques. The public should also be able to learn the rules that govern when, where, and against whom such techniques may be used, including when a warrant or other authorization must be obtained in order to use particular techniques. To the extent that law enforcement agencies have adopted rules to limit the retention or use of information collected using hacking techniques, or have procedures in place to address any damage to the security or integrity of target systems, the public should know what those safeguards are.

As it stands, almost none of this information is available publicly. In order to promote government accountability and public oversight – and to ensure compliance with domestic and international law – we request the agency disclose information regarding its use and regulation of hacking and related social engineering techniques.

II. Records Requested

For purposes of all requests below, the phrases "hacking techniques" and "equipment, software and/or technology that implements or facilitates hacking techniques" have their ordinary meanings, as described in the background section above, and include (but are not limited to):

> (1) techniques that have been described by the government using terms such as "Network Investigation Technique" or "NIT," "Computer Network Exploitation" or "CNE," "Computer and Internet Protocol Address Verifier" or "CIPAV," "Internet Protocol Address Verifier" or "IPAV", "Remote Access Search and Surveillance" or "RASS," "Remote Computer Search," "Remote Access Search," "Remote Search," "Web Bug," "Sniffer," "Computer Tracer," "Internet Tracer," "Remote Computer

[25] *See, e.g.*, 18 U.S.C. § 2703(d) (providing for court ordered disclosure of certain stored computer files or communications without probable cause on a showing of mere relevance to an investigation).

[26] *See, e.g.*, 18 U.S.C. § 2703(c)(2).

Trace," "lawful hacking," "extraordinary access," "equipment interference," "Trojan horse," and "Magic Lantern;"

(2) software commonly described as malware, spyware, trojans, worms, or viruses;

(3) hacking software created by commercial or government entities, as described above (*see supra* notes 8–19 and accompanying text); and/or

(4) social engineering techniques that facilitate hacking including phishing/spear phishing, watering hole attacks (*i.e.*, serving malware to all visitors of a website or other internet location), and encouraging or requesting that companies provide the government access to their users' private data by creating and/or installing software on user devices.

We hereby request the following records:[27]

1. **Records relating to the agency's use, acquisition, borrowing, sale, loan, research, and/or development of hacking techniques or equipment, software and/or technology that implements or facilitates hacking techniques including, but not limited to:**
    a. **Purchase orders, lease agreements, invoices, receipts and/or contracts with entities providing such equipment, software and/or technology;**
    b. **Policies, guidelines, legal opinions and/or rules;**
    c. **Documents requiring or requesting that information regarding hacking techniques be kept confidential;**
    d. **Deployment and/or training materials, including materials from internal and external conferences, courses, training sessions, workshops, or similar events;**
    e. **Marketing, promotional, or informational materials, including materials from external conferences, trade shows, training sessions, workshops, or similar events that employees of the agency have attended.**

2. **Records that constitute or contain reports, audits, assessments, or statistical information about hacking techniques or law enforcement investigations in which a hacking technique was deployed.**

---

[27] For purposes of this request, "records" should be given the broadest possible definition including, but not limited to, letters, reports, final drafts of legal and policy memoranda, guidance documents, instructions, notes, communications, training materials, formal and informal presentations, technical manuals, technical specifications, purchase orders, contracts, agreements, memoranda of understanding, confidentiality or nondisclosure agreements, tape recordings, electronic records (including email, data, and computer source and object code), and any other materials in the agency's possession.

3. **Records reflecting internal approvals or authorizations (or disapprovals/denials) of the use of a hacking technique in a criminal or civil investigation, as well any standard forms, templates, checklists or similar documents that are used as part of any internal process(es) for obtaining approval to use hacking techniques.**

4. **Licenses, waivers, or agreements with local, state and/or federal agencies or foreign entities, including foreign law enforcement agencies, that concern the use of hacking techniques.**

5. **Communications with local, state and/or federal agencies or foreign entities, including foreign law enforcement agencies, that concern "computer network exploitation" or a "network investigative technique."**

We request that responsive records be provided electronically in their native file format, wherever possible. *See* 5 U.S.C. § 552(a)(3)(B). Alternatively, we request that the records be provided electronically in text-searchable PDF, in the best image quality in the agency's possession, and in separate, Bates-stamped files.

III. Request for Expedited Processing

Privacy International, the ACLU, and CLTC seek expedited processing of this request pursuant to 5 U.S.C. § 552(a)(6)(E). Expedited processing is appropriate because there is a "compelling need" for the information requested, and because the information is urgently needed by organizations "primarily engaged in disseminating information" in order to inform the public about actual or alleged government activity. 5 U.S.C. § 552(a)(6)(E)(v)(II).

A. PI, the ACLU, and CLTC are organizations primarily engaged in disseminating information in order to inform the public about actual or alleged government activity.

PI, the ACLU, and CLTC are "primarily engaged is disseminating information . . . to the public" within the meaning of the statute.[28] 5 U.S.C. § 552(a)(6)(E)(v)(II). PI is a non-profit organization that researches and investigates government surveillance to ensure that such surveillance is consistent with the rule of law, international human rights law, and relevant domestic laws.[29] PI's core mission therefore involves raising awareness about laws,

[28] *See also* 22 C.F.R. § 171.11(f)(2); 32 C.F.R. § 286.8(e)(1)(i)(B); 15 C.F.R. § 2004.6(d)(2)(ii); 32 C.F.R. § 286.8(e)(1)(i)(B); 32 C.F.R. §1700.12(c)(2).

[29] *See* Privacy International, *About Privacy International*, https://privacyinternational.org/about (last visited July 18, 2018).

policies and technologies that place privacy at risk to ensure that the public is informed and engaged. PI uses the information it obtains through its investigations, including through FOIA requests, in order to publish reports, press releases, and other materials to inform the public.[30]

PI publishes in-depth reports regarding a broad range of privacy and surveillance issues.[31] PI also publishes country reports on the state of privacy and surveillance issues in particular jurisdictions around the world.[32] In doing this work, PI engages in original investigative research, which it synthesizes and publishes for public consumption. For example, PI engaged in a years-long effort to gather information about surveillance products offered for sale by private companies at trade shows, ultimately compiling that information and making it readily available through its Surveillance Industry Index and an accompanying report.[33] PI has also published reports specifically on the topic of government hacking.[34]

---

[30] For examples of these materials, see Privacy International, *Investigation and Research*, https://privacyinternational.org/how-we-fight/investigation-and-research (last visited July 18, 2018); Privacy International, *Campaigns and Communications*, https://privacyinternational.org/how-we-fight/campaigns-and-communications (last visited July 18, 2018).

[31] *See, e.g.*, Privacy International, *Fintech: Privacy and Identity in the New Data-Intensive Financial Sector* (Nov. 2017), https://privacyinternational.org/sites/default/files/2017-12/Fintech%20report.pdf; Privacy International, *Smart Cities: Utopian Vision, Dystopian Reality* (Oct. 2017), https://privacyinternational.org/sites/default/files/2017-12/Smart%20Cities-Utopian%20Vision%2C%20Dystopian%20Reality.pdf; Privacy International, *The Global Surveillance Industry* (July 2016), https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf; Privacy International, *Aiding Surveillance* (Nov. 1, 2013), https://privacyinternational.org/sites/default/files/2017-12/Aiding%20Surveillance.pdf; Privacy International, *A Race to the Bottom – Privacy Ranking on Internet Service Companies* (June 2007), https://privacyinternational.org/sites/default/files/2017-12/A_Race_Bottom.pdf.

[32] Privacy International, *State of Privacy*, https://privacyinternational.org/type-resource/state-privacy.

[33] *See* Privacy International, *Monitoring the Surveillance Industry: Using Data to Protect Privacy* (Aug. 2, 2016), https://privacyinternational.org/feature/811/monitoring-surveillance-industry-using-data-protect-privacy; Surveillance Industry Index, https://sii.transparencytoolkit.org/; Privacy International, *The Global Surveillance Industry* (July 2016), https://www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

[34] *See* Privacy International, *Pay No Attention to the Man Behind the Curtain: Exposing and Challenging Government Hacking for Surveillance* (June 2018) https://privacyinternational.org/sites/default/files/2018-06/Pay%20No%20Attention%20to%20That%20Man%20Behind%20the%20Curtain%20-%20Exposing%20and%20Challenging%20Government%20Hacking%20for%20Surveillance.pdf; Privacy International, *Hacking Safeguards and Legal Commentary* (June 11, 2018), https://privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary.

In addition to subject-matter and country reports, PI also publishes explainers on a variety of privacy and surveillance issues, including government hacking.[35] It also frequently publishes opinion and commentary on its own blog and other news outlets.[36]

PI plans to analyze the information gathered through this Request and publish its findings in order to educate the public about the privacy implications of government hacking techniques. The records requested are not sought for commercial use, and the Requesters plan to disseminate the information obtained in response to this Request to the public at no cost.

Similarly, the ACLU is "primarily engaged in disseminating information." 5 U.S.C. § 552(a)(6)(E)(v)(II). Obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public are critical and substantial components of the ACLU's work and are among its primary activities. *See ACLU v. DOJ*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).[37]

The ACLU regularly publishes *STAND*, a print magazine that reports on and analyzes civil liberties-related current events. The magazine is disseminated to over 980,000 people. The ACLU also publishes regular updates and alerts via email to over 3.1 million subscribers (both ACLU members and non-members). These updates are additionally broadcast to over 3.8 million social media followers. The magazine as well as the email and social-media alerts often include descriptions and analysis of information obtained through FOIA requests.

The ACLU also regularly issues press releases to call attention to documents obtained through FOIA requests, as well as other breaking news,[38] and ACLU attorneys are

---

[35] *See* Privacy International, Explainers, https://privacyinternational.org/type-resource/explainers; Privacy International, *Video: Government Hacking 101*, https://privacyinternational.org/video/2068/video-government-hacking-101.

[36] *See, e.g.*, Privacy International, *Can Governments Really Hack Your Webcam?* (Oct. 20, 2017), https://privacyinternational.org/blog/643/can-governments-really-hack-your-webcam; Privacy International, *In Defense of Offensive Hacking Tools* (May 2, 2017), https://privacyinternational.org/blog/849/defense-offensive-hacking-tools; Privacy International, *Hacking Team Spyware Sold to US DEA, US Army* (April 15, 2015), https://privacyinternational.org/blog/1463/hacking-team-spyware-sold-us-dea-and-us-army.

[37] Courts have found that the ACLU as well as other organizations with similar missions that engage in information-dissemination activities similar to the ACLU are "primarily engaged in disseminating information." *See, e.g.*, *Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005); *ACLU*, 321 F. Supp. 2d at 29 n.5; *Elec. Privacy Info. Ctr. v. DOD,* 241 F. Supp. 2d 5, 11 (D.D.C. 2003).

[38] *See, e.g.*, Press Release, American Civil Liberties Union, U.S. Releases Drone Strike 'Playbook' in Response to ACLU Lawsuit (Aug. 6, 2016), https://www.aclu.org/news/us-releases-drone-strike-playbook-response-aclu-lawsuit; Press Release, American Civil Liberties Union, Secret Documents Describe Graphic Abuse and Admit Mistakes (June 14, 2016), https://www.aclu.org/news/cia-releases-dozens-torture-documents-response-aclu-lawsuit; Press Release, American Civil Liberties Union, U.S. Releases Targeted

interviewed frequently for news stories about documents released through ACLU FOIA requests.[39]

Similarly, the ACLU publishes reports about government conduct and civil liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA requests. This material is broadly circulated to the public and widely available to everyone for no cost or, sometimes, for a small fee. ACLU national projects regularly publish and disseminate reports that include a description and analysis of government documents obtained through FOIA requests.[40] The ACLU also regularly publishes books, "know your rights" materials, fact sheets, and educational brochures and pamphlets designed to educate the public about civil liberties issues and government policies that implicate civil rights and liberties.

The ACLU publishes a widely read blog where original editorial content reporting

---

Killing Memo in Response to Long-Running ACLU Lawsuit (June 23, 2014), https://www.aclu.org/national-security/us-releases-targeted-killing-memo-response-long-running-aclu-lawsuit; Press Release, American Civil Liberties Union, Justice Department White Paper Details Rationale for Targeted Killing of Americans (Feb. 4, 2013), https://www.aclu.org/national-security/justice-department-white-paper-details-rationale-targeted-killing-americans; Press Release, American Civil Liberties Union, Documents Show FBI Monitored Bay Area Occupy Movement (Sept. 14, 2012), https://www.aclu.org/news/documents-show-fbi-monitored-bay-area-occupy-movement-insidebayareacom.

[39] *See, e.g.*, Cora Currier, *TSA's Own Files Show Doubtful Science Behind Its Behavioral Screen Program*, The Intercept, Feb. 8, 2017, https://theintercept.com/2017/02/08/tsas-own-files-show-doubtful-science-behind-its-behavior-screening-program/ (quoting ACLU attorney Hugh Handeyside); Karen DeYoung, *Newly Declassified Document Sheds Light on How President Approves Drone Strikes,* Wash. Post, Aug. 6, 2016, http://wapo.st/2jy62cW (quoting former ACLU deputy legal director Jameel Jaffer); Catherine Thorbecke, *What Newly Released CIA Documents Reveal About 'Torture' in Its Former Detention Program,* ABC, June 15, 2016, http://abcn.ws/2jy40d3 (quoting ACLU attorney Dror Ladin); Nicky Woolf, *US Marshals Spent $10M on Equipment for Warrantless Stingray Device*, Guardian, Mar. 17, 2016, https://www.theguardian.com/world/2016/mar/17/us-marshals-stingray-surveillance-airborne (quoting ACLU attorney Nate Wessler); David Welna, *Government Suspected of Wanting CIA Torture Report to Remain Secret,* NPR, Dec. 9, 2015, http://n.pr/2jy2p71 (quoting ACLU project director Hina Shamsi).

[40] *See, e.g.*, Hugh Handeyside, *New Documents Show This TSA Program Blamed for Profiling Is Unscientific and Unreliable — But Still It Continues* (Feb. 8, 2017, 11:45 AM), https://www.aclu.org/blog/speak-freely/new-documents-show-tsa-program-blamed-profiling-unscientific-and-unreliable-still; Carl Takei, *ACLU-Obtained Emails Prove that the Federal Bureau of Prisons Covered Up Its Visit to the CIA's Torture Site* (Nov. 22, 2016, 3:15 PM), https://www.aclu.org/blog/speak-freely/aclu-obtained-emails-prove-federal-bureau-prisons-covered-its-visit-cias-torture; Brett Max Kaufman, *Details Abound in Drone 'Playbook' – Except for the Ones That Really Matter Most* (Aug. 8, 2016, 5:30 PM), https://www.aclu.org/blog/speak-freely/details-abound-drone-playbook-except-ones-really-matter-most; Nathan Freed Wessler, *ACLU- Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida* (Feb. 22, 2015, 5:30 PM), https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida; Ashley Gorski, *New NSA Documents Shine More Light into Black Box of Executive Order 12333* (Oct. 30, 2014, 3:29 PM), https://www.aclu.org/blog/new-nsa-documents-shine-more-light-black-box-executive-order-12333; ACLU, *ACLU Eye on the FBI: Documents Reveal Lack of Privacy Safeguards and Guidance in Government's "Suspicious Activity Report" Systems* (Oct. 29, 2013), https://www.aclu.org/sites/default/files/assets/eye_on_fbi_-_sars.pdf.

on and analyzing civil rights and civil liberties news is posted daily.[41] The ACLU creates and disseminates original editorial and educational content on civil rights and civil liberties news through multi-media projects, including videos, podcasts, and interactive features.[42] The ACLU also publishes, analyzes, and disseminates information through its heavily visited website, www.aclu.org. The website addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The ACLU's website also serves as a clearinghouse for news about ACLU cases, as well as analysis about case developments, and an archive of case-related documents. Through these pages, and with respect to each specific civil liberties issue, the ACLU provides the public with educational material, recent news, analyses of relevant Congressional or executive branch action, government documents obtained through FOIA requests, and further in-depth analytic and educational multi-media features.

The ACLU website includes many features on information obtained through the FOIA.[43] For example, the ACLU's "Predator Drones FOIA" webpage, https://www.aclu.org/national-security/predator-drones-foia, contains commentary about the ACLU's FOIA request, press releases, analysis of the FOIA documents, numerous blog posts on the issue, documents related to litigation over the FOIA request, frequently asked questions about targeted killing, and links to the documents themselves. Similarly, the ACLU maintains an online "Torture Database," a compilation of over 100,000 pages of FOIA documents that allows researchers and the public to conduct sophisticated searches of FOIA documents relating to government policies on rendition, detention, and interrogation.[44]

---

[41] *See* https://www.aclu.org/blog.

[42] *See* https://www.aclu.org/multimedia.

[43] *See, e.g.*, Nathan Freed Wessler & Dyan Cortez, *FBI Releases Details of 'Zero-Day' Exploit Decisionmaking Process* (June 26, 2015, 11:00 AM), https://www.aclu.org/blog/free-future/fbi-releases-details-zero-day-exploit-decisionmaking-process; Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights; *ACLU v. DOJ – FOIA Case for Records Relating to the Killing of Three U.S. Citizens*, ACLU Case Page, https://www.aclu.org/national-security/anwar-al-awlaki-foia-request; *ACLU v. Department of Defense*, ACLU Case Page, https://www.aclu.org/cases/aclu-v-department-defense; *Mapping the FBI: Uncovering Abusive Surveillance and Racial Profiling*, ACLU Case Page, https://www.aclu.org/mappingthefbi; *Bagram FOIA*, ACLU Case Page https://www.aclu.org/cases/bagram-foia; *CSRT FOIA*, ACLU Case Page, https://www.aclu.org/national-security/csrt-foia; *ACLU v. DOJ – Lawsuit to Enforce NSA Warrantless Surveillance FOIA Request*, ACLU Case Page, https://www.aclu.org/aclu-v-doj-lawsuit-enforce-nsa-warrantless-surveillance-foia-request; *Patriot FOIA*, ACLU Case Page, https://www.aclu.org/patriot-foia; *NSL Documents Released by DOD*, ACLU Case Page, https://www.aclu.org/nsl-documents-released-dod?redirect=cpredirect/32088.

[44] *The Torture Database*, ACLU, https://www.thetorturedatabase.org; *see also Countering Violent Extremism FOIA Database*, ACLU, https://www.aclu.org/foia-collection/cve-foia-documents; *TSA Behavior*

The ACLU has also published a number of charts and explanatory materials that collect, summarize, and analyze information it has obtained through the FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA requests—the ACLU created an original chart that provides the public and news media with a comprehensive summary index of Bush-era Office of Legal Counsel memos relating to interrogation, detention, rendition, and surveillance.[45] Similarly, the ACLU produced an analysis of documents released in response to a FOIA request about the TSA's behavior detection program;[46] a summary of documents released in response to a FOIA request related to the FISA Amendments Act;[47] a chart of original statistics about the Defense Department's use of National Security Letters based on its own analysis of records obtained through FOIA requests;[48] and an analysis of documents obtained through FOIA requests about FBI surveillance flights over Baltimore.[49]

The ACLU plans to analyze, publish, and disseminate to the public the information gathered through this Request. The records requested are not sought for commercial use and the requesters plan to disseminate the information disclosed as a result of this Request to the public at no cost.

Finally, CLTC is likewise "primarily engaged in disseminating information." 5 U.S.C. § 552(a)(6)(E)(v)(II). CLTC's mission is to press for greater transparency and accountability in government through litigation and policy advocacy.[50] CLTC works in its own name and on behalf of clients to obtain and disseminate information on issues involving technology & privacy, law enforcement accountability, national security, veterans, and related issues. For example, CLTC has gathered and disseminated information on issues

---

Detection FOIA Database, ACLU, https://www.aclu.org/foia-collection/tsa-behavior-detection-foia-database; *Targeted Killing FOIA Database*, ACLU, https://www.aclu.org/foia-collection/targeted-killing-foia-database.

[45] *Index of Bush-Era OLC Memoranda Relating to Interrogation, Detention, Rendition and/or Surveillance*, ACLU (Mar. 5, 2009), https://www.aclu.org/sites/default/files/pdfs/safefree/olcmemos_2009_0305.pdf.

[46] *Bad Trip: Debunking the TSA's 'Behavior Detection' Program*, ACLU (2017), https://www.aclu.org/sites/default/files/field_document/dem17-tsa_detection_report-v02.pdf.

[47] *Summary of FISA Amendments Act FOIA Documents Released on November 29, 2010*, ACLU, https://www.aclu.org/files/pdfs/natsec/faafoia20101129/20101129Summary.pdf.

[48] *Statistics on NSL's Produced by Department of Defense*, ACLU, https://www.aclu.org/other/statistics-nsls-produced-dod.

[49] Nathan Freed Wessler, *FBI Documents Reveal New Information on Baltimore Surveillance Flights* (Oct. 30, 2015, 8:00 AM), https://www.aclu.org/blog/free-future/fbi-documents-reveal-new-information-baltimore-surveillance-flights.

[50] *See* Civil Liberties & Transparency Clinic, About the Clinic, http://www.law.buffalo.edu/beyond/clinics/civil-liberties.html.

including attempted suicides at local county jails, improper courtroom sealing practices, toxic chemical exposures to servicemembers from open-air burn pits in Iraq and Afghanistan, and other issues.[51] CLTC has affirmatively published reports and op-eds regarding its work[52] and has obtained significant media coverage as well.[53] Like PI and the ACLU, CLTC seeks the records here not for any commercial use and plans to analyze and publish the information for the public's benefit.

Under well-established case-law these activities clearly establish that PI, the ACLU, and CLTC all qualify as organizations "primarily engaged in disseminating information" within the meaning of 5 U.S.C. § 552(a)(6)(E)(v)(II). *See ACLU v. DOJ,* 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding that a non-profit, public-interest group that "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that to an audience" is "primarily engaged in disseminating information") (internal citation omitted); *see also Leadership Conference on Civil Rights v. Gonzales,* 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (finding Leadership Conference – whose mission is "to serve as the site of record for relevant and up-to-the-minute civil rights news and information" and to "disseminate[] information regarding civil rights and voting rights to educate the public [and] promote effective civil rights laws" – to be "primarily engaged in the dissemination of information").[54]

B. The records sought are urgently needed to inform the public about actual or alleged government activity.

Second, a "compelling need" exists in this case because there is an "urgency to inform the public about actual or alleged federal government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II); 28 C.F.R. § 16.5(d). This Request is made to further the public's understanding of law enforcement agencies' deployment of hacking and related social engineering techniques to access and gather information on computer systems. This is an urgent and emerging issue of broad concern to the public. Numerous breaking news stories

---

[51] *See* Civil Liberties & Transparency Clinic, Current Projects, http://www.law.buffalo.edu/beyond/clinics/civil-liberties.current-projects.html.

[52] See, *e.g.*, Laura Gardiner, Andy Plewinski & Amanda S. Wadsworth, *Sealed Cases, Sealed Documents, Sealed Opinions*, Wash. Post. Volokh Conspiracy Blog, July 6, 2017, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/07/06/sealed-cases-sealed-documents-sealed-opinions/?utm_term=.7c6e6932ae40.

[53] *See generally* Civil Liberties & Transparency Clinic, In the News, http://www.law.buffalo.edu/beyond/clinics/civil-liberties.in-the-news.html.

[54] Even if one or two of the co-requesters is found not to be "primarily engaged in disseminating information," expedited processing should be granted if another co-requester qualifies. "[A]s long as one of the plaintiffs qualifies as an entity 'primarily engaged in disseminating information,' this requirement is satisfied." *ACLU v. DOJ*, 321 F. Supp. 2d at 30 n. 5 (citing *Al-Fayed v. CIA*, 254 F.3d 300, 309 (D.C. Cir. 2001)).

have recently been published concerning the government's use of hacking.[55] The Department of Justice's Office of Inspector General recently released a report assessing the accuracy of the FBI's public statements concerning its capabilities to hack into a cell phone.[56]

Disclosure on an expedited basis is necessary in order to inform this public discussion and debate. Without access to the information sought here regarding law enforcement agencies' ongoing use of hacking, the public will remain in the dark about the legality of these techniques, their impact on personal privacy, and the unintended consequences that result from the government interfering with computer systems to access and gather information.

For these reasons, and on the basis of all of the facts provided in this Request, expedited processing should be granted. The undersigned certify, pursuant to 5 U.S.C. § 552(a)(6)(E)(vi), that the information provided is true and correct to the best of their knowledge and belief.

IV. Request for a Public Interest Fee Waiver

PI, the ACLU, and CLTC are entitled to a waiver of search, review and duplication fees because disclosure of the information requested is in the public interest as defined in 5 U.S.C. § 552(a)(4)(a)(iii); 28 C.F.R. § 16.10(k). A waiver or reduction of fees is allowed under these sections if (1) furnishing the information "is likely to contribute significantly to public understanding of the operations or activities of the government agency" and (2) "is not primarily in the commercial interest of the requester." 5 U.S.C. § 552(a)(4)(a)(iii); 28 C.F.R. § 16.10(k); *see also, e.g.*, *Tripp v. Department of Defense,* 193 F. Supp. 2d 229, 242 (D.D.C. 2002). A fee waiver must be granted if both of these requirements are met. *See Fitzgibbon v. Agency for Intern. Development*, 724 F.Supp.1048, 1050 (D.D.C. 1989).

---

[55] *See* Cox, *The DEA Met with Controversial iPhone Hackers NSO Group*, *supra* note 15; Ryan Cooper, *The NSA Needs to Stop Hacking*, The Week, Nov. 14, 2017, http://theweek.com/articles/736984/nsa-needs-stop-hacking; Jennifer Granick, *Challenging Government Hacking: What's at Stake*, American Civil Liberties Union, Nov. 2, 2017, https://www.aclu.org/blog/privacy-technology/internet-privacy/challenging-government-hacking-whats-stake; Lisa Vaas, *It is Not OK to Break the Law to Catch Criminals, Judge Rules*, Naked Security, June 8, 2017, https://nakedsecurity.sophos.com/2017/06/08/it-is-not-ok-to-break-the-law-to-catch-criminals-judge-rules/; Charlie Savage, *Amid Trump Inquiry, a Primer on Surveillance Practices and Privacy*, New York Times, Mar. 24, 2017, https://www.nytimes.com/2017/03/24/us/politics/primer-on-surveillance-practices-and-privacy.html; Feliz Solomon, *The CIA Just Published its Updated Rules on Citizen Surveillance*, Time, Jan. 19, 2017, http://time.com/4638866/cia-surveillance-nsa-intelligence/; Joseph Cox, *The FBI Spent $775K on Hacking Team's Spy Tools Since 2011*, Wired, July 8, 2015, https://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/.

[56] See Office of the Inspector General for the U.S. Department of Justice, Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation, March 2018, https://oig.justice.gov/reports/2018/o1803.pdf.

This Request meets the first prong because, as discussed above, PI, the ACLU, and CLTC will use the information sought herein to educate the public about the government's use and regulation of hacking for surveillance purposes, including its adherence to internal guidelines, federal law, and international law. The disclosure of information regarding such operations is in the public interest because the government's surveillance powers, capabilities and activities are matters of great public interest and concern. This interest is reflected in relevant media coverage of these issues.[57] For example, in January 2017, *Time Magazine* published an article titled, *The CIA Just Published its Updated Rules on Citizen Surveillance*. The author notes, "The public has become increasingly frustrated with the secrecy and spread of government surveillance programs."[58] And in March 2017, *The New York Times* published a *Primer on Surveillance Practices and Privacy*, confirming public interest in government surveillance, particularly in the context of the new administration."[59]

There exist major gaps in the public record about government hacking for investigative purposes. Thus, while we now know that various agencies are spending millions on software and hardware capable of capturing our private activities and communications, we still do not know the rules governing the deployment of these techniques.[60] Without further information, the public is left in the dark regarding the scope of these activities; what rules agencies must follow; and whether they in fact follow these rules. These questions are critical with respect to such potentially intrusive technology. This Request seeks to fill these significant gaps in the public record.

This Request also meets the second prong of the test for a public interest fee waiver because disclosure here is not in any way in the "commercial interest of the requester." 5 U.S.C. § 552(a)(4)(a)(iii); 28 C.F.R. § 16.10(k). PI, the ACLU, and CLTC are all non-profit organizations that have no commercial interest in the disclosure of the requested records. PI, the ACLU, and CLTC do not intend to sell this information and will receive no financial gain from it. Rather, any information obtained through this request will be disseminated to the public at no cost for the purpose of educating the public and promoting the protection of civil liberties and human rights. In making this request, PI, the ACLU, and CTLC are not acting for their own (or any other) commercial interest.

For these reasons, we request that all search, review and duplication fees related to the Request be waived in full. 5 U.S.C. § 552(a)(4)(a)(iii).

---

[57] See *id.*

[58] Solomon, The CIA Just Published its Updated Rules on Citizen Surveillance, *supra* note 55.

[59] Savage, Amid Trump Inquiry, a Primer on Surveillance Practices and Privacy, *supra* note 55.

[60] *See, e.g.*, Cox, The DEA Met with Controversial iPhone Hackers NSO Group, *supra* note 15.

V. Request for a Waiver of Search and Review Fees

In the event that the public interest waiver of all fees is not granted, PI, the ACLU, and CLTC request a waiver of search and review fees because PI and the ACLU qualify as "representative[s] of the news media," CLTC qualifies as an "educational institution," and the records are not sought for "commercial use," within the meaning of 5 U.S.C. § 552(a)(4)(A)(ii); 28 C.F.R. 16.10(b). *See* 28 C.F.R. 16.10(c)(1)(i), 16.10(c)(3), 16.10(d)(1) (search and review fees shall not be charged to representatives of the news media or educational institutions). Therefore, fees associated with the processing of the Request should be "limited to reasonable standard charges for document duplication." 5 U.S.C. § 552(a)(4)(A)(ii)(II). Moreover, we request that all records be produced electronically, thereby eliminating duplication costs altogether wherever possible. In any event, reasonable fees shall exclude charges for the first 100 pages. *See* 28 C.F.R. 16.10(d)(4)(1).

PI and the ACLU qualify as "representative[s] of the news media," because each organization is an "entity that actively gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience." 5 U.S.C. § 552(a)(4)(A)(ii); 28 C.F.R. 16.10(b)(6). *See also Nat'l Sec. Archive v. DOD*, 880 F.2d 1381, 1387 (D.C. Cir. 1989) (finding that an organization that gathers information, exercises editorial discretion in selecting and organizing documents, "devises indices and finding aids," and "distributes the resulting work to the public" is a "representative of the news media" for purposes of the FOIA); *Serv. Women's Action Network v. DOD*, 888 F. Supp. 2d 282 (D. Conn. 2012) (requesters, including ACLU, were representatives of the news media and thus qualified for fee waivers for FOIA requests to the Department of Defense and Department of Veterans Affairs); *ACLU of Wash. v. DOJ*, No. C09–0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding that the ACLU of Washington is an entity that "gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience"); *ACLU*, 321 F. Supp. 2d at 30 n.5 (finding non-profit public interest group to be "primarily engaged in disseminating information"). Further, "news" is defined as "information that is about current events or that would be current to the public." 28 C.F.R. 16.10(b)(6).

For the reasons discussed above, PI and the ACLU both qualify as representatives of the news media because they each conduct research on a variety of issues related to privacy and surveillance and publish their research in a variety of formats, which are freely available to the public. For the same reasons that PI and the ACLU are "primarily engaged in the dissemination of information," they are each a "representative of the news media." *See supra* § III.A.

Indeed, other organizations whose mission, functioning, publishing, and public education activities are similar in kind to those of PI and the ACLU's are "regularly granted news representative status." *See, e.g., Serv. Women's Action Network v. Dep't of Def.*, 888 F. Supp. 2d 282, 287 (D. Conn. 2012). Courts have determined that such organizations are "representative[s] of news media." *See, e.g.*, *Ctr. for Pub. Integrity v. HHS, No*. 06-1818, 2007 WL 2248071, at *5 (D.D.C. Aug. 3, 2007). *Cause of Action v. IRS*, 125 F. Supp. 3d 145 (D.C. Cir. 2015); *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d at 10–15 (finding non-profit public interest group that disseminated an electronic newsletter and published books was a "representative of the news media" for purposes of the FOIA); *Nat'l Sec. Archive*, 880 F.2d at 1387; *Judicial Watch, Inc. v. DOJ*, 133 F. Supp. 2d 52, 53–54 (D.D.C. 2000) (finding Judicial Watch, self-described as a "public interest law firm," a news media requester).[61]

On account of these factors, fees associated with responding to FOIA requests are regularly waived for the ACLU as a "representative of the news media."[62] As was true in those instances, the ACLU and PI meet the requirements for a fee waiver here.

Additionally, co-requester CLTC qualifies as an "educational . . . institution" entitled to a limitation of fees under 5 U.S.C. § 552(a)(4)(A)(II)(ii). An "educational institution" is defined as "any school that operates a program of scholarly research." 28 C.F.R. § 16.10(b)(4). CLTC is a part of the University at Buffalo School of Law, a law school accredited by the American Bar Association.[63] CLTC seeks this information in furtherance

---

[61] Courts have found these organizations to be "representatives of the news media" even though they engage in litigation and lobbying activities beyond their dissemination of information/public education activities. *See, e.g.*, *Elec. Privacy Info. Ctr.*, 241 F. Supp. 2d 5; *Nat'l Sec. Archive*, 880 F.2d at 1387; s*ee also Leadership Conference on Civil Rights*, 404 F. Supp. 2d at 260; *Judicial Watch, Inc.*, 133 F. Supp. 2d at 53–54.

[62] In August 2017, CBP granted a fee-waiver request regarding a FOIA request for records relating to a muster sent by CBP in April 2017. In May 2017, CBP granted a fee-waiver request regarding a FOIA request for documents related to electronic device searches at the border. In April 2017, the CIA and the Department of State granted fee-waiver requests in relation to a FOIA request for records related to the legal authority for the use of military force in Syria. In March 2017, the Department of Defense Office of Inspector General, the CIA, and the Department of State granted fee-waiver requests regarding a FOIA request for documents related to the January 29, 2017 raid in al Ghayil, Yemen. In May 2016, the FBI granted a fee-waiver request regarding a FOIA request issued to the DOJ for documents related to Countering Violent Extremism Programs. In April 2013, the National Security Division of the DOJ granted a fee-waiver request with respect to a request for documents relating to the FISA Amendments Act. Also in April 2013, the DOJ granted a fee-waiver request regarding a FOIA request for documents related to "national security letters" issued under the Electronic Communications Privacy Act. In August 2013, the FBI granted the fee-waiver request related to the same FOIA request issued to the DOJ. In June 2011, the DOJ National Security Division granted a fee waiver to the ACLU with respect to a request for documents relating to the interpretation and implementation of a section of the PATRIOT Act. In March 2009, the State Department granted a fee waiver to the ACLU with regard to a FOIA request for documents relating to the detention, interrogation, treatment, or prosecution of suspected terrorists.

[63] University at Buffalo School of Law, Fast Facts & ABA-Required Disclosures, www.law.buffalo.edu/about/consumer-information.html#accredidaton (last visited Sep. 6, 2018).

of its programmatic and scholarly focus on investigating and obtaining transparency about law enforcement uses of technologies and related issues.[64] Therefore, CLTC qualifies as an "educational institution" for purposes of FOIA and is entitled to a limitation of fees. Fees for this Request should be limited on this basis even if you determine that PI and the ACLU are not entitled to a limitation of fees as representatives of the news media.

If fees are not waived and exceed $100, we ask that you contact us.

* * *

Please furnish all responsive records to the following email address or mailing address:

Jonathan Manes
Civil Liberties & Transparency Clinic
University at Buffalo School of Law
507 O'Brian Hall, North Campus
Buffalo, NY 14260-1100
(716) 645-6222
jmmanes@buffalo.edu

If the Request is denied in whole or in part, we ask that all denials be justified by reference to specific FOIA exceptions pursuant to 5 U.S.C. § 552(a)(6)(A)(i). We further expect the release of all segregable portions of otherwise exempt material. We reserve the right to appeal a decision to withhold any information or to deny a waiver or limitation of fees.

If you have any questions or concerns, please do not hesitate to contact us using the information below. We expect a response regarding our request for expedited processing within ten days, 5 U.S.C. § 552(a)(6)(E)(2)(i), and a response to other aspects of the request within the twenty working-day statutory time limit, 5 U.S.C. § 552(a)(6)(A)(i).

[64] Civil Liberties and Transparency Clinic, About the Clinic, www.law.buffalo.edu/beyond/clinics/civil-liberties.html (last visited Sep. 6, 2018).

Thank you for your prompt attention to this matter.

Sincerely,

Brett Max Kaufman
Vera Eidelman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
bkaufman@aclu.org
veidelman@aclu.org

Jennifer Stisa Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
Tel: 415.343.0758
jgranick@aclu.org

Jonathan Manes, *supervising attorney*
Alex Betschen, *student attorney*
RJ McDonald, *student attorney*
Colton Kells, *student attorney*
Civil Liberties and Transparency Clinic[65]
University at Buffalo School of Law, SUNY
507 O'Brian Hall, North Campus
Buffalo, NY 14260-1100
Tel: 716.645.6222
jmmanes@buffalo.edu

Scarlet Kim
Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom
Tel: +44 (0)203 422 4321
scarlet@privacyinternational.org

[65] This FOIA request was prepared in substantial part by former student attorneys Laura Gardiner, Patrick Hoover, Thora Knight, Cindy Manuele, and Suzanne Starr.